NASA
Technical
Paper
2105

December 1982

Generation of Pseudo-Random Numbers

Leonard W. Howell and
Mario H. Rheinfurth

NASA

NASA
Technical
Paper
2105

1982

Generation of Pseudo-Random Numbers

Leonard W. Howell and
Mario H. Rheinfurth
George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama

National Aeronautics
and Space Administration

**Scientific and Technical
Information Branch**

TABLE OF CONTENTS

GENERATION OF PSEUDO-RANDOM NUMBERS

I. INTRODUCTION

The advent of high-speed digital computers has made it possible to use simulation techniques incorporating probabilistic features. These simulations are generally referred to as Monte Carlo simulations and are resorted to whenever the systems being studied are not amenable to deterministic analytical methods or where direct experimentation is not feasible. An integral part of these simulations is the use of random numbers having a certain specified distribution characteristic of the process being studied. Since these simulations require a vast amount of calculations, speed is a vitally important factor. It was soon recognized that it was intractable to fill the computer's memory with large aggregates of random numbers. Because of this, computer algorithms were developed which allowed random numbers to be generated on-line. Since the generation of random numbers by such numerical algorithms is somewhat a contradiction in terms, they are often called "pseudo-random" numbers. There are essentially two problems encountered in generating such random numbers. One is that the generated random numbers are not representative of the desired distribution, and the other is that they are not statistically random, i.e., that there exist correlations in the generated numbers. The latter problem is the more serious one as evidenced by the considerable attention it has been given in the literature.

This report presents several random number generators which have been found particularly useful in aerospace engineering applications. APL computer programs are also listed in Appendix B for most of the generators.

II. UNIFORM RANDOM NUMBER GENERATORS

The basic element of all Monte Carlo simulations is the uniform random number generator. Once uniform random numbers are available, all other desired distributions can be obtained either by use of the probability integral transformation or by applying some known relationship between the desired distribution to be generated and the uniform distribution.[1] One of the early methods used to generate uniform random numbers was the mid-square method originally proposed by John V. Neumann. In practice, one selects an arbitrary K-digit number, squares it, and then selects the K middle digits as the new random number. The process is repeated using this new random number. The drawback of this method is that it can produce a zero random number at unpredictable times and, thus, the process terminates. Consequently, this method was abandoned quite early in favor of the so-called congruential method first proposed by D. H. Lehmer in 1949 [1]. Accordingly, the random number generator takes the form

1. Often it is convenient to generate a random number from a specified distribution by employing its relationship to the normal distribution. However, one must first generate the normal random number(s) as a function of uniform random numbers and then proceed to the desired distribution.

$$X_{i+1} \equiv (a\, X_i + b) \text{ Mod } M \quad , \tag{1}$$

where the multiplier a, increment b, and modulus M are integers. The starting value X_o is called the "seed" of the random number generator. Since the congruential relationship (1) is cyclical, the sequence of random numbers will repeat after a certain period. Generators in which b = 0 are called multiplicative; otherwise, they are called mixed. The statistical behavior of the generated random numbers is predominantly governed by the choice of the multiplier a and the modulus M. Therefore, the most widely used generators are of the multiplicative type (b = 0). Many empirical and theoretical tests have been developed to assess the "goodness" of a random number generator. One of the most popular of these tests today is the lattice test which determines the lattice structure of the random number generator by comparing successive n-tuples $(x_i, x_{i+1}, \ldots, x_{i+n-1})$ and $(x_{i+1}, x_{i+2}, \ldots, x_{i+n})$. According to this test an acceptable generator can be obtained by selecting the constants a, b, and M to achieve a nearly hyper-cubic lattice structure, i.e., the ratio of cell sides should be close to unity [2]. In practice, n is usually less than or equal to five [3]. Especially useful are congruential generators for which the modulus M is a prime number and hence, are called prime modulus generators. If the multiplier a is selected to be a primitive root modulo M, the generated random number sequence attains its maximum period P = M-1 and all possible value from 0 to M-1 will be generated.

Two useful uniform random number generators of this type which have very satisfactory lattice structures are:

$$a = 7^5 = 16{,}807 \quad , \quad b = 0 \quad , \quad M = 2^{31}-1 = 2{,}147{,}483{,}647 \quad , \tag{2}$$

with 5-dimensional cell side ratios 1:7.60:3.39:2.09:1.67, and

$$a = 7^{602{,}479} \text{ Mod}(2^{31}-1) = 29{,}903{,}947 \quad , \quad b = 0 \quad , \quad \text{and}$$

$$M = 2^{31}-1 = 2{,}147{,}483{,}647 \quad , \tag{3}$$

with 5-dimensional cell side ratios: 1:1.04:1.30:1.22:1.09 [4].

III. RANDOM NUMBERS FROM CONTINUOUS DISTRIBUTIONS

Many of the generators for continuous distributions are obtained by a direct application of the probability integral transformation [5]. For a given uniform random number u between zero and one, a random number x having the desired distribution F(x) is obtained by solving the equation u = F(x) for x. Since this process requires the determination of the inverse cumulative distribution function $F^{-1}(x)$, its practicality depends upon the availability of explicit expressions or convenient approximations for this inverse cumulative distribution function. We now discuss methods on how to generate random numbers from continuous distributions which appear frequently in aerospace engineering simulations.

A. The Normal Distribution

The most common distribution is the normal or Gaussian distribution with density function given by

$$f(x;\mu,\sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \quad , \quad -\infty < x, \ \mu < \infty \quad \text{and} \quad \sigma > 0 \quad . \tag{4}$$

Consequently, a variety of methods have been devised which can be used to generate normal random numbers. Of these, the following three were found to be satisfactory and practical in terms of accuracy and computer run time.

1. Hastings Approximation

This method invokes the probability integral transformation in a slight variation in that it employs the complement of the cumulative distribution $Q(x) = 1-F(x)$. The reason for this is that suitable rational approximations for $Q(x)$ were derived by Hastings [6]. The most accurate of Hastings approximations is given as:

$$x = t - \frac{C_o + C_1 t + C_2 t^2}{1 + d_1 t + d_2 t^2 + d_3 t^3} + \varepsilon(p) \tag{5}$$

where

$C_o = 2.515517$

$C_1 = 0.802853$

$C_2 = 0.010328$

$d_1 = 1.432788, \ t = \sqrt{-2\ln p}$

$d_2 = 0.189269, \ 0 \le p \le 0.5$

$d_3 = 0.001308$, and $|\varepsilon(p)| \le 4.5 \times 10^{-5}$

X is the desired Normal random number and p is a uniform random number.

2. Box-Mueller or "Polar" Method

This method generates a pair of normal random variables using a pair of uniform random numbers as follows:

Let u_1 and u_2 be independent uniform random variables and define

$$x_1 = (-2\ln u_1)^{1/2} \cos 2\pi u_2 \quad ,$$
$$x_2 = (-2\ln u_1)^{1/2} \sin 2\pi u_2 \quad . \tag{6}$$

Then x_1 and x_2 are two independent normal random variables with zero mean and unit variance. To see this, we establish the inverse relationships

$$u_1 = e^{-\frac{(x_1^2 + x_2^2)}{2}}$$

and (7)

$$u_2 = \frac{-1}{2\pi} \tan^{-1}\left(\frac{x_2}{x_1}\right) \quad .$$

It follows then that the joint probability density function of x_1,x_2 is

$$f\,(x_1,x_2) = \frac{1}{2\pi}\, e^{-\frac{(x_1^2 + x_2^2)}{2}} = f(x_1)\; f(x_2) \quad , \tag{8}$$

and, thus, the desired conclusions, including the independence of x_1 and x_2, are obtained [7].

3. Central Limit Method

Let x_1, x_2, ..., x_n be a sequence of n uniform random variables. Then

$$y_n = \left(\frac{n}{12}\right)^{-1/2}\left(\sum_{i=1}^{n} x_i - n/2\right) \quad , \tag{9}$$

will be distributed asymptotically as a normal random variable with zero mean and unit variance. For n = 12, we see that (9) reduces to

$$y_{12} = \sum_{i=1}^{12} x_i - 6 \quad .$$

The exact distribution of the standardized sum of n independent uniform random numbers can be easily derived using moment generating functions. Since the sum x of n independent uniform variables has moment generating function

$$\phi_x(t) = \frac{1}{t^n} (1 - e^{-t})^n \quad , \tag{10}$$

its density function is given as

$$f(x) = \frac{1}{(n-1)!} \sum_{k=0}^{n} (-1)^k \binom{n}{k} [(x-k)\ u(x-k)]^{n-1} \quad , \tag{11}$$

where

$$u(s) = \begin{cases} 0 & s \leq 0 \\ 1 & s > 0 \end{cases} \qquad \text{and} \qquad 0 \leq x \leq n \quad .$$

For the standardized random variable y_n in equation (9), we find that

$$f_{y_n}(y) = \left(\frac{n}{12}\right)^{1/2} \frac{1}{(n-1)!} \sum_{k=0}^{n} (-1)^k \binom{n}{k} \left[\left(\left(\frac{n}{12}\right)^{1/2} y + \frac{n}{2} - k\right) u\left(\left(\frac{n}{2}\right)^{1/2} y + \frac{n}{2} - k\right)\right]^{n-1} \quad , \tag{12}$$

where $-\sqrt{3n} \leq y \leq \sqrt{3n}$.

Density functions obtained by this method for n = 2, 4, 12, 20 are compared with the normal density function (dotted) in Figure 1. Also, a comparison of the cumulative distribution function for n = 12 with the cumulative normal distribution is given in Table 1 to four decimal places.

The agreement between the two distributions is very good except in the tail areas. But a comparison of random numbers generated by the three methods revealed no significant statistical differences even for the tail areas.

A comparison of computer CPU run times for each of these three methods to generate 1000 normal random numbers is as follows:

Method	Time
Hastings Approximation	1.13 sec
Box-Mueller	1.02 sec
Central Limit Method	1.08 sec

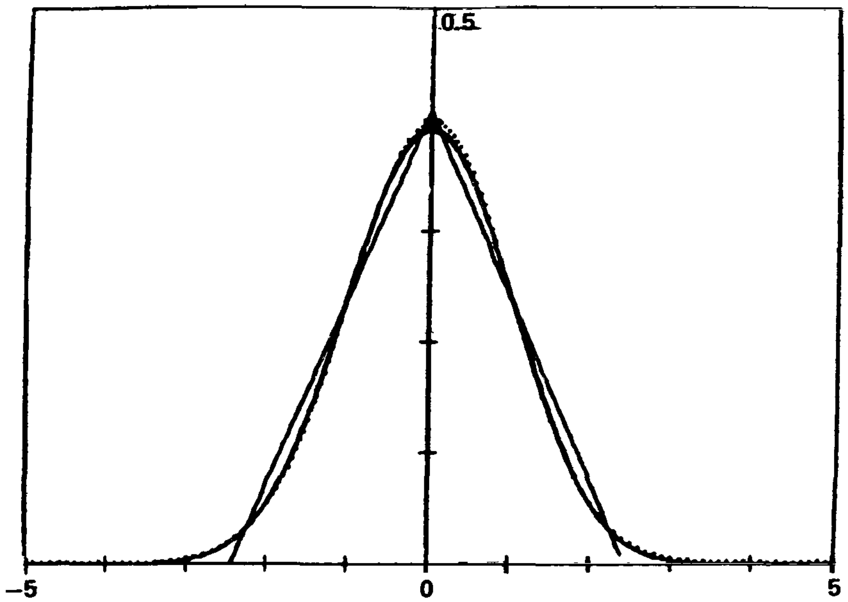

Figure 1. Normal density function (dotted) and standardized sum of uniforms (n = 2, 4, 12, 20).

TABLE 1. CUMULATIVE NORMAL DISTRIBUTION

x	F(x)	$F_{C.L.}(x)$
-4.0	3.167×10^{-4}	8.526×10^{-6}
-3.5	2.326×10^{-4}	1.212×10^{-4}
-3.0	1.350×10^{-3}	1.007×10^{-3}
-2.5	6.210×10^{-3}	5.579×10^{-3}
-2.0	2.275×10^{-2}	2.227×10^{-2}
-1.5	6.681×10^{-2}	6.745×10^{-2}
-1.0	1.587×10^{-1}	1.608×10^{-1}
-0.5	3.085×10^{-1}	3.106×10^{-1}
0.0	5.000×10^{-1}	5.000×10^{-1}
0.5	6.915×10^{-1}	6.894×10^{-1}
1.0	8.413×10^{-1}	8.393×10^{-1}
1.5	9.332×10^{-1}	9.326×10^{-1}
2.0	9.773×10^{-1}	9.777×10^{-1}
2.5	9.938×10^{-1}	9.944×10^{-1}
3.0	9.987×10^{-1}	9.990×10^{-1}
3.5	9.998×10^{-1}	9.999×10^{-1}
4.0	1.000	1.000

*Comparison of the cumulative normal distribution F(x) with the cumulative distribution function for the central limit method using equation (13) as the *density function with n = 12.*

B. Log-Normal Distribution

It is often claimed that the log-normal distribution is as fundamental as the normal distribution and may be thought of as arising from the combination of random terms by a multiplicative process. The log-normal distribution has been applied in a wide variety of fields including social sciences, physical sciences, and engineering and its density function is given by

$$f(x;\mu,\sigma) = (2\pi\sigma^2 x^2)^{-1/2} \exp\left[-1/2\left(\frac{\ln x - \mu}{\sigma}\right)^2\right], \quad \begin{array}{l} 0 < x,\ \sigma < \infty \\ -\infty < \mu < \infty \end{array}, \tag{13}$$

Log-normal random numbers x may be generated by the relationship $x = e^y$, where y is a normal random number obtained by methods discussed in Section III, paragraph A.

C. Weibull Distribution

The Weibull distribution is perhaps the most popular distribution at the present time when dealing with problems of reliability and material fatigue. Its appeal stems from its mathematical tractability and for this reason is often preferred to the gamma distribution. The Weibull density function is given by

$$f(x;\alpha,\beta) = \alpha\beta\, x^{\beta-1} \exp(-\alpha x^{\beta}) \quad , \quad 0 \le x < \infty \qquad \alpha,\beta > 0 \quad . \tag{14}$$

The cumulative distribution function $F(x) = 1 - e^{-\alpha x^\beta}$ leads immediately to the inverse relationship

$$x = \left(\frac{-\alpha}{\ln u}\right)^{\beta} \tag{15}$$

as the desired Weibull random generator.

D. Gamma Distribution

The gamma distribution is another two parameter distribution which is also quite flexible in fitting a variety of random processes. It finds use in reliability analysis, meteorology, and aerospace engineering. Its density function is

$$f(x) = \frac{\alpha^{\beta}}{\Gamma(\beta)}\, e^{-\alpha x}\, x^{\beta-1} \tag{16}$$

where $0 \le x < \infty$ and $\alpha,\beta > 0$.

For integer values of β, the gamma distribution is often referred to as the Erlangian distribution after the Danish mathematician, A. K. Erlang, who introduced it in the theory of queues and Markov processes in 1917. Random numbers following the Erlangian distribution are generated by the formula

$$x = -\frac{1}{\alpha}\sum_{i=1}^{\beta} \ln u_i \quad . \tag{19}$$

E. Exponential Distribution

The exponential distribution appears often in engineering applications because of its importance in reliability theory and queueing theory. The probability density function of the exponential distribution is

$$f(x;\alpha) = \alpha e^{-\alpha x} \quad , \tag{20}$$

where $x, \alpha > 0$. In this case, an explicit expression for the inverse cumulative distribution function is easily obtained by solving the equation $u = 1 - e^{-\alpha x}$ for x, producing

$$x = -\frac{\ln u}{\alpha} \tag{21}$$

as the desired exponential random number generator.

F. Chi-Square Distribution

As a special case of the gamma distribution, the χ^2-distribution is often used as a measure of goodness of fit of a specified distribution to observed frequencies. For discrete variates, χ^2 provides a sensitive test of departure from the Poisson distribution. The Chi-Square density function with n degrees of freedom is given by

$$f(x;n) = \frac{x^{n-1} e^{-x/2}}{2^n \Gamma(n)} \quad , \qquad x > 0 \quad \text{and} \quad n = 1,2,3,\ldots \quad . \tag{22}$$

Because of its relationship to the normal distribution, Chi-Square random numbers may be generated by taking the sum of n squared Normal random numbers.

G. F Distribution

The F distribution appears extensively in statistical hypothesis testing under normality theory and has the density function

$$f(x;m,n) = \frac{n^{n/2}\, m^{m/2}\, \Gamma\left(\frac{m+n}{2}\right)}{\Gamma(n/2)\, \Gamma(m/2)} \frac{x^{n/2\,-\,1}}{(m + nx)^{1/2(m+n)}} , \tag{23}$$

where $x > 0$ and $m,n = 1,2,\ldots,$ are degrees of freedom. In practice, it is generally found to be most convenient to make use of the F distribution's relationship to the Chi-Square distribution in order to generate F random numbers. That is, if $\chi^2(m)$ and $\chi^2(n)$ are two independent Chi-Square random variables with m and n degrees of freedom, respectively, then

$$Y = \frac{\chi^2(m)/m}{\chi^2(n)/n} \tag{24}$$

follows the F-distribution with m, n degrees of freedom. Thus,

$$Y = \frac{\frac{1}{m}\sum_{i=1}^{m} X_i^2}{\frac{1}{n}\sum_{i=m+1}^{m+n} X_i^2} \tag{25}$$

is the desired F random number generator with m and n degrees of freedom and the X_i, $i = 1,2,\ldots,m+n$ are Normal random numbers.

H. Beta Distribution

To generate random numbers from the Beta distribution with density function given by:

$$f(x;\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\,\Gamma(\beta)}\, x^{\alpha-1}\,(1-x)^{\beta-1} \quad , \quad 0 < x < 1 \quad , \quad 0 < \alpha,\beta < \infty, \tag{26}$$

it is most convenient to make use of a relationship between the Beta distribution and the F-distribution. That is, if X is a random variable following the F distribution with m and n degrees of freedom, then $Y = \frac{1}{1 + m/n\, X}$ follows the Beta distribution. Consequently,

$$Y = \frac{\sum_{i=1}^{2m} X_i^2}{\sum_{i=1}^{2m} X_i^2 + \sum_{i=2m+1}^{2n+2m} X_i^2} \qquad (27)$$

is the desired Beta random numbers generator, where the X_i's are standard Normal random numbers realized by methods in Section III, paragraph A.

IV. RANDOM NUMBERS FROM DISCRETE DISTRIBUTIONS

Generation of random numbers from a discrete distribution is handled in a manner analogous to that of a continuous distribution. Given a uniform random number u and cumulative discrete distribution F(x), the least value of x for which $F(x) \geq u$ is sought. This x is the desired random number having discrete density function f(x).

A. Binomial Distribution

The cumulative binominal distribution is given by

$$F(x;n,p) = \sum_{k=0}^{x} \binom{n}{k} p^k (1 - p)^{x-k} \quad . \qquad (28)$$

For a given uniform number u, one may successively evaluate the upper limit x until the minimum value of x is found for which

$$\sum_{k=0}^{x} \binom{n}{k} p^k (1 - p)^{n-k} \geq u \quad . \qquad (29)$$ [2]

An alternate method is based on the sum of n independent Bernoulli random variables. By this method, Bernoulli trials, each having probability of success p, are simulated with each Bernoulli trial being assigned a one or zero (depending on success or failure).

---

2. Because factorials, exponentials, and powers frequently occur in probability density functions, care must be taken to avoid computer overflows/underflows when computing individual components of the density function. Recursive relationships are quite useful in dealing with these types of problems, but computer programs employing recursive relationships are, in general, much slower.

Then the sum of these n Bernoulli random numbers will be a random number from a Binomial population with parameters n and p. However, it was found that this process is relatively slow.

B. Poisson Distribution

Poisson random numbers x may be generated from cumulative distribution function

$$F(x;\lambda) = \sum_{k=0}^{x} \frac{\lambda^k e^{-\lambda}}{k!} \quad , \quad \lambda > 0 \quad , \tag{30}$$

by using the same technique which was used for the binominal distribution. An alternate method for obtaining Poisson random numbers is by generating uniform random numbers u_i until the inequality

$$\prod_{i=1}^{k+1} u_i < e^{-\lambda} \tag{31}$$

is satisfied, which gives k as the desired Poisson random number. However, this method was found to be relatively slow.

C. Neyman Type-A and Thomas Distributions

These two distributions belong to the category of cluster (self-exciting) point processes and have found application in aerospace engineering, ecology, reliability, and forestry. Cluster processes are characterized by a primary (mother) process which generates at each point secondary (daughter) events. When only daughter events appear in the final process and when primary and secondary distributions are both Poisson, the resulting distribution is known as the Neyman type-A counting distribution with probability function [8]

$$p(n;\alpha,\beta) = \sum_{m=0}^{\infty} \frac{(\alpha m)^n e^{-\alpha m}}{n!} \frac{\beta^m e^{-\beta}}{m!} \quad , \quad n = 0,1,2,\ldots \text{ and } \alpha,\beta > 0 \quad . \tag{32}$$

The parameter β represents the rate at which primary events occur and α is the average number of secondary counts per primary. The mean and variance is $\alpha\beta$ and $(1 + \alpha)\alpha\beta$, respectively. The Thomas distribution is similar, except that primary events are counted in the final process. The probability function is given by

$$p(n;\alpha,\beta) = \sum_{m=0}^{n} \frac{(\alpha m)^{n-m}}{(n-m)!} e^{-\alpha m} \frac{\beta^m e^{-\beta}}{m!} \quad , \quad n = 0, 1, 2, \ldots \quad , \tag{33}$$

with mean $(1 + \alpha)\beta$ and variance $(1 + 3\alpha + \alpha^2)\beta$.

APL programs are provided in Appendix B which generate random numbers from these distributions.

V. CONCLUSION

Because large scale simulations often require a vast number of random numbers from various distributions, emphasis should be placed on speed and accuracy of the methods used. We have found the congruential uniform generators presented in this report to be both suitable and practical. However, not all possibilities have been exhausted and the literature is found to be extensive in this area. Random numbers can be generated from nonuniform distributions by finding the inverse to the cumulative distribution functions in accordance with the probability integral transformation. However, when no convenient inverse exists, numerical approximation methods or statistical relationships may be used to generate the desired random numbers. Again, speed and accuracy should be key factors in choosing between candidate methods. Some useful approximations to the cumulative normal distribution are given in Appendix A and APL programs for most of the generators are listed in Appendix B.

APPENDIX A

APPROXIMATION TO THE CUMULATIVE NORMAL DISTRIBUTION

Because of the extensive application of the Normal distribution in aerospace simulation studies, we include here three methods for approximating the cumulative standard Normal distribution. Other useful formulae may be found in Reference 9. Denote the standard normal density function by

$$f(x) = (2\pi)^{-1/2} e^{-x^2/2}$$

and its cumulative distribution function by F(x). Then F(x) may be represented by each of the following:

$$\frac{1}{2} + \frac{1}{\sqrt{2\pi}} \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{2^n n! \ (2n+1)} \ , \qquad -\infty < x < \infty \qquad \text{(A-1)}$$

$$1 - f(x) \left[\frac{1}{x+} \frac{1}{x+} \frac{2}{x+} \frac{3}{x+} \cdots \right], \qquad x > 0 \qquad \text{(A-2)}$$

$$\frac{1}{2} + f(x) \left[\frac{x^2}{1-} \frac{x^2}{3+} \frac{2x^2}{5-} \frac{3x^2}{7+} \frac{4x^2}{9-} \cdots \right. , \qquad x \geq 0 \qquad \text{(A-3)}$$

The last two formulae are called continued fractions, where the conventional notation

$$\frac{a_1}{b_1+} \frac{a_2}{b_2+} \cdots = \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \ddots}}}$$

is used to conserve space. Since each formula is exact, we investigate their rates of convergence to F(x) for computational convenience.

Equation A-2 converges most rapidly for $x \geq 3$ while A-1 and A-3 are preferred for $0 < x < 3$.

APPENDIX B

APL PROGRAMS

```
     ∇ R←N CDFI CDF
[1]    R←⍳0
[2]    L:R←R,+/CDF<UNF 1
[3]    →(0<N←N-1)/L
[4]    →0
[5]    ⍝ RETURNS N RANDOM NUMBERS FROM THE
[6]    ⍝ DISCRETE DISTRIBUTION FUNCTION
[7]    ⍝ SPECIFIED BY CDF.
     ∇

     ∇ R←CTRALIM N
[1]    R←¯6+(+/¯1+?N⍴1001)÷1000;N←N,12
[2]    →0
[3]    ⍝ THIS FUNCTION GENERATES NORMAL
[4]    ⍝ RANDOM NUMBERS ACCORDING TO
[5]    ⍝ THE CENTRAL LIMIT METHOD.
     ∇

     ∇ P←K CUMNORM X;C;S;Y;A;M;T;Z;S0
[1]    C←(○2)*¯0.5;Y←S←S0←X;A←1+K×2;M←0
[2]    L0:T←X×X×Z×¯1*⌊Z←1+K-M←M+1
[3]    A←(2×Z)+¯1+T÷A
[4]    S←S+S0←S0×-X×X×(¯1+2×M)÷M×2×1+2×M
[5]    Y←X+Z÷Y
[6]    →(M<K)/L0
[7]    P←0 0 0
[8]    P[1]←1-C×(*-X×X÷2)÷Y
[9]    P[2]←0.5+C×(*-X×X÷2)×X÷A
[10]   P[3]←0.5+C×S
[11]   →0
[12]   ⍝ THREE FORMULAE FROM THE HANDBOOK OF MATHEMATICAL
[13]   ⍝ FUNCTIONS, EDITED BY ABROMOWITZ, 1970 , ARE PROVIDED.
[14]   ⍝ THE FIRST TWO ARE CONTINUED FRACTIONS AND THE THIRD IS
[15]   ⍝ A POWER SERIES. P[1] (EQ. 26.2.14, PAGE 932, GIVES
[16]   ⍝ P(X), X>0. P[2] ALSO GIVES P(X) AND IS EQ. 26.2.15.
[17]   ⍝ P[3] IS EQ. 26.2.10.  [1] CONVERGES MOST RAPIDLY FOR
[18]   ⍝ X≥3 WHILE P[2] AND P[3] ARE PREFERRED FOR 0<X<3.
[19]   ⍝ PROGRAMMED BY L. HOWELL, 19 MAY 82.
     ∇

     ∇ E←PARAM GENLOGNORM N;MU;VAR
[1]    VAR←PARAM[2];MU←PARAM[1]
[2]    E←*MU+(VAR*0.5)×NORM N
[3]    →0
[4]    ⍝ GENERATES N LOG-NORMAL RANDOM
[5]    ⍝ NUMBERS WITH PARAMETERS MU AND
[6]    ⍝ VAR (MU AND VAR ARE THE MEAN
[7]    ⍝ AND VARIANCE OF THE DEFINING NORMAL
[8]    ⍝ DISTRIBUTION).
     ∇
```

```
    ∇ R←HASTING N;C;D;U0;NU;DE;T
[1]   C←2.515517 0.802853 0.010328;D←1 1.432788 0.189269 0.001308
[2]   U0←¯0.5001+(?Nρ1000)÷1000
[3]   T←(-2×⍟|U0)*0.5
[4]   NU←C[1]+T×C[2]+T×C[3]
[5]   DE←D[1]+T×D[2]+T×D[3]+T×D[4]
[6]   R←(×U0)×(T-NU÷DE)
[7]   →0
[8]   ⍝ GENERATES NORMAL RANDOM NUMBERS
[9]   ⍝ USING HASTING'S RATIONAL APPROXIMATIONS
    ∇
```

```
    ∇ CDF←W NEYMAN A;II;J;M;X;Y;N;NP;R;S
[1]   NP←*-W×1-*-A
[2]   N←0
[3]   L1:N←N+1;S←⍳0;M←0
[4]   L2:X←1;M←1+M
[5]   II←1
[6]   L3:X←X×A×M÷N+1-II
[7]   →(N≥II←II+1)/L3
[8]   X←X×*-A×M
[9]   Y←1;J←1
[10]  L4:Y←Y×W÷M+1-J
[11]  →(M≥J←J+1)/L4
[12]  Y←Y×*-W
[13]  S←S,X×Y
[14]  →((R<0)∨(R>1E¯12)∨(M≤5))/L2;R←-/¯2↑S
[15]  NP←NP,+/S
[16]  →(0.999>+/NP)/L1
[17]  CDF←+\NP
[18]  →0
[19]  ⍝ COMPUTES THE CUMULATIVE NEYMAN-TYPE-A
[20]  ⍝ PROBABILITY DISTRIBUTION FUNCTION.
[21]  ⍝ W IS AVERAGE NO. OF PRIMARY(MOTHER) EVENTS
[22]  ⍝ A IS AVERAGE NO. OF SECONDARY(DAUGHTER) EVENTS PER PRIMARY
[23]  ⍝ PROGRAMMED BY LEONARD HOWELL, AUGUST 4, 1982.
    ∇
```

```
    ∇ R←NORM S
[1]   R←¯6+0.0001×+/?Sρ10000;S←S,12
    ∇
```

```
     ∇ PDF←PDFFRCDF CDF;Y
[1]    PDF←CDF-Y;Y←0,1↓¯1⌽CDF
     ∇

     ∇ CDF←POISSON ST;P0;P;K
[1]    CDF←P0←*-ST
[2]    K←P←1
[3]    L0:P←P×ST÷K
[4]    CDF←CDF,(¯1↑CDF)+P×P0
[5]    K←K+1
[6]    →(0.9999>¯1↑CDF)/L0
[7]    →0
[8]    ⍝ RETURNS THE CUMULATIVE POISSON
[9]    ⍝ DISTRIBUTION FUNCTION WITH
[10]   ⍝ PARAMETER ST.
     ∇

     ∇ R←MU POIS1 K;F;X
[1]    R←(*-MU)×(MU*X)÷!X←0,⍳K
[2]    F←+\R
[3]    →0
[4]    ⍝ CUM. DIST. FUNCT. FOR POISSON
     ∇

     ∇ R←MU POIS2 K;F1;P;X
[1]    X←0;P←R←(*-MU);
[2]    L:P←MU×P÷X←X+1
[3]    R←R,P
[4]    →(K≠X)/L
[5]    F1←+\R
     ∇


     ∇ R←POLAR N
[1]    R←(?R)÷R←(2,⌈×/N,0.5)⍴1073741824
[2]    R←N⍴(1 2∘.○(○2)×¯1 0↓R)×(¯2 ¯2∘.×⍟1 0↓R)*0.5
[3]    →0
[4]    ⍝ GENERATES RANDOM NUMBERS USING
[5]    ⍝ THE BOX-MUELLER METHOD, OFTEN
[6]    ⍝ REFERRED TO AS THE POLAR METHOD.
     ∇

     ∇ R←NP RBINO1 N;A;I;U;K
[1]    R←⍳0
[2]    L0:A←0;I←0
[3]    L:U←(¯1+?1001)÷1000
[4]    K←U≥NP[2]
[5]    A←A+K
[6]    →(NP[1]≥I←I+1)/L
[7]    R←R,A
[8]    →(0≠N←N-1)/L0
[9]    →0
     ∇
```

```
     ∇ R←NP RBINO2 N;F;M;P;PF;U;X;Y
[1]    X←0,⍳M;M←NP[1];P←NP[2]
[2]    PF←(X!M)×(P*X)×(1-P)*M-X
[3]    F←+\PF
[4]    U←(¯1+?Nρ1001)÷1000
[5]    R←+/U∘.>F
[6]    →0
[7]    ⍝ GENERATES BINOMIAL RANDOM NUMBERS
[8]    ⍝ USING THE INVERSE METHOD.
[9]    ⍝ NP[1] IS THE SAMPLE SIZE AND
[10]   ⍝ NP[2) IS THE PROBABILITY
     ∇

     ∇ R←NP RBINO3 N;M;P;U
[1]    M←NP[1];P←NP[2]
[2]    U←(¯1+?(N,M)ρ1001)÷1000
[3]    R←+/U≥P
[4]    →0
[5]    ⍝ GENERATES BINOMIAL RANDOM NUMBERS
[6]    ⍝ AS THE SUM OF BERNOULLI TRIALS.
[7]    ⍝ NP[1] IS THE SAMPLE SIZE AND
[8]    ⍝ NP[2] IS THE PROBABILITY.
     ∇


     ∇ R←MU RPOIS3 N;A;I;K;U
[1]    R←⍳0;I←1
[2]    L0:A←1;K←0
[3]    L:U←(¯1+?1001)÷1000
[4]    A←A×U
[5]    K←K+1
[6]    →(A≥(*-MU))/L
[7]    R←R,(¯1+K)
[8]    →(N≥I←I+1)/L0
[9]    →0
[10]   ⍝ GENERATES POISSON RANDOM NUMBERS
[11]   ⍝ BY TAKING THE PRODUCT OF UNFORM
[12]   ⍝ RANDOM NUMBERS AND CHECKING FOR
[13]   ⍝ FOR THE INEQUALITY EXP(-MEAN)
     ∇

     ∇ R←MU RPOIS4 N;X;A;P;F;U;M
[1]    X←0;A←P←(*-MU)
[2]    L:A←MU×A÷X←X+1
[3]    P←P,A
[4]    →(X≠⌈M←MU+4×MU*0.5)/L
[5]    P←P,A
[6]    F←+\P
[7]    U←(¯1+?Nρ1001)÷1000
[8]    R←+/U∘.>F
[9]    →0
[10]   ⍝ USES THE INVERSE CUMULATIVE
[11]   ⍝ METHOD FOR DISCRETE RANDOM
[12]   ⍝ NUMBERS.
```

```
      ∇STDUNFSUM[⎕]∇
    ∇ STDUNFSUM N;K;X;S;Z;PRT;Y;UX;SIG;X1;U
[1]   UX←N÷2;SIG←(N÷12)*0.5
[2]   X←-UX÷SIG;K←¯1+⍳(N+1);Y←⍳0;PRT←⍳0
[3]   L:Z←(X1-K)×U←X1>K;X1←UX+SIG×X
[4]   S←SIG×(-/(K!N)×Z*N-1)÷!(N-1)
[5]   Y←Y,S
[6]   PRT←PRT,X
[7]   X←X+0.05
[8]   →(X≤UX÷SIG)/L
[9]   0 DRAW Y VS PRT
[10]  →0
[11]  ⍝ COMPUTES THE PROBABILITY DENSITY
[12]  ⍝ FUNCTION OF THE STANDARDIZED
[13]  ⍝ SUM OF N INDEPENDENT UNIFORM
[14]  ⍝ RANDOM VARIABLES BY TAKING THE
[15]  ⍝ INVERSE OF ITS MOMENT GEN-
[16]  ⍝ ERATING FUNCTION. PROGRAMMED
[17]  ⍝ BY LEONARD HOWELL 08/04/82.
    ∇


      ∇STUDENT[⎕]∇
    ∇ T←V STUDENT P;C;D;R;XP;G1;G2;G3;G4;G;VP;D1;D2
[1]   C←2.515517 0.802853 0.010328;D←1 1.432788 0.189269 0.001308
[2]   R←(¯2×⍟P)*0.5;VP←V*¯1 ¯2 ¯3 ¯4
[3]   XP←R-D1÷D2;D1←+/C×R*0 1 2;D2←+/D×R*0 1 2 3
[4]   G1←(+/XP*3 1)÷4
[5]   G2←(+/(XP*5 3 1)×5 16 3)÷96
[6]   G3←(+/3 19 17 ¯15×XP*7 5 3 1)÷384
[7]   G4←(+/79 776 1482 ¯1920 ¯945×XP*9 7 5 3 1)÷92160
[8]   G←G1,G2,G3,G4
[9]   T←XP++/G×VP
[10]  →0
[11]  ⍝ THIS FUNCTION APPROXIMATES THE INVERSE STUDENT-T
[12]  ⍝ DISTRIBUTION AND IS USEFUL IN AUTOMATIC LOOK-UP OF
[13]  ⍝ CRITICAL VALUES IN HYPOTHESIS TESTING.  FORMULA
[14]  ⍝ 26.7.5, PAGE 949 OF ABRAMOWITZ'S HANDBOOK OF
[15]  ⍝ MATHEMATICAL FUNCTIONS IS USED IN CONJUNCTION WITH
[16]  ⍝ FORMULA 26.2.23 (APPROXIMATES THE INVERSE NORMAL
[17]  ⍝ DISTRIBUTION), PAGE 933.  PROGRAMMED BY L. HOWELL,
[18]  ⍝  JUNE 23, 1982.
    ∇
```

```
      ∇THOMAS[⎕]∇
    ∇ CDF←THOMAS INP;M;D;E;ED;I;J;P;T;IJ;J1
[1]   M←INP[1]⍝ AV NO OF MOTHER EVENTS(PER MS)
[2]   D←INP[2]⍝ AV NO OF DAUGHTER EVENTS (COUNTS)
[3]   E←(*-M)×1,M
[4]   T←E[1]
[5]   CDF←E[1],E[1]+E[2]×ED←*-D
[6]   I←2
[7]   L1:P←J←1
[8]   E←E,(¯1↑E)×M÷I
[9]   L2:P←P×D÷J
[10]  →(I>J←J+1)/L2
[11]  P←P×ED
[12]  T←P×E[2]
[13]  J←1
[14]  L3:P←P×((J1÷J)*IJ)×IJ×ED÷D×J1←J+1;IJ←I-J
[15]  T←T+P×E[J+2]
[16]  →(I>J←J+1)/L3
[17]  CDF←CDF,(¯1↑CDF)+T
[18]  I←I+1
[19]  →(0.9999>¯1↑CDF)/L1
[20]  →0
[21]  ⍝ RETURNS THE CUMULATIVE THOMAS DISTRIBUTION
    ∇

      ∇UNF[⎕]∇
    ∇ U←UNF S;N
[1]   U←⍳0;N←×/S
[2]   L:U←U,UNFD×UNFX←UNFM|UNFR×UNFX
[3]   →(0<N←N-1)/L
[4]   U←S⍴U
[5]   →0
[6]   ⍝ STANDARD UNIFORM NUMBER GENERATOR
    ∇

      ∇UNFIC[⎕]∇
    ∇ UNFIC SEED
[1]   UNFM←2147483647
[2]   UNFR←29903947
[3]   UNFX←SEED
[4]   UNFD←÷UNFM
[5]   →0
[6]   ⍝ INITIALIZES PARAMETERS FOR THE
[7]   ⍝ STANDARD UNIFORM GENERATOR.
    ∇
```

```
      ∇UNFSUM[⎕]∇
    ∇ UNFSUM N;K;X;S;Z;U;PRT;Y
[1]   X←0;K←¯1+⍳(N+1);Y←⍳0;PRT←⍳0
[2]   L:Z←(X-K)×U←X>K
[3]   S←(-/(K!N)×Z*N-1)÷!(N-1)
[4]   Y←Y,S
[5]   PRT←PRT,X
[6]   X←X+0.1
[7]   →(X≤N)/L
[8]   0 DRAW Y VS PRT-N÷2
[9]   ⍝ COMPUTES INVERSE OF THE MOMENT
[10]  ⍝ GENERATING FUNCTION OF THE SUM OF
[11]  ⍝ INDEPENDENT UNIFORM VARIABLES
    ∇

      ∇UNIFORM[⎕]∇
    ∇ R←M UNIFORM N;I;U;A;S
[1]   R←⍳0;I←1;U←SEED;A←16807;MOD←¯1+2*31
[2]   L:U←MOD|A×U
[3]   S←⌈M×U÷MOD
[4]   R←R,S
[5]   →(N≥I←I+1)/L
[6]   →0
[7]   ⍝ STANDARD UNIFORM NUMBER GENERATOR.
    ∇
```

REFERENCES

1. Lehmer, D. H.: Proc. 2nd Symposium on Large-Scale Digital Computing Machinery. Cambridge, Harvard University Press, 1948, pp. 141-146.

2. Marsaglia, G.: The Structure of Linear Congruential Sequences; Applications of Number Theory to Numerical Analysis. S. K. Zaremba (ed.), Academic Press, 1972.

3. Atkinson, A. C.: Test of Pseudo-random Numbers. Applied Statistics, Vol. 29, No. 2, pp. 164-171.

4. Carroll, Stan N.: Aerospace Engineer, Dynamics and Trajectory Analysis Branch, Control Systems Div., Systems Dynamics Lab., MSFC, NASA, Huntsville, AL, personal communication, 1982.

5. Harris, B.: Theory of Probability, Addison-Wesley, 1966.

6. Hastings, C.: Approximations for Digital Computers. Princeton University Press, Princeton, N.J., 1955.

7. Box, G. E. P. and Mueller, M. E.: A Note on the Generation of Random Normal Deviates. Ann. Math. Statist., Vol. 29, pp. 610-611.

8. Neyman, J. and Scott, E. L.: Processes of Clustering and Applications, in Stochastic Point Processes: Statistical Analysis, Theory, and Applications, P.A. W. Lewis (ed.), Wiley-Interscience, New York, 1972, pp. 646-681.

9. Abramowitz, M. and Stegun, I. A.: Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. National Bureau of Standards, Applied Mathematics Series, 55, U. S. Government Printing Office, Washington, 1964.

BIBLIOCRAPHY

Aitchison, J. and Brown, J. A.: The Lognormal Distribution. Cambridge University Press, 1963.

Feller, William: An Introduction to Probability Theory and Its Applications. Vol. 1, Wiley, 1964.

Hahn, G. J. and Shapiro, S. S.: Statistical Models in Engineering. Wiley, 1967.

1. REPORT NO. NASA TP-2105	2. GOVERNMENT ACCESSION NO.	3. RECIPIENT'S CATALOG NO.
4. TITLE AND SUBTITLE Generation of Pseudo-Random Numbers		5. REPORT DATE December 1982
		6. PERFORMING ORGANIZATION CODE
7. AUTHOR(S) Leonard W. Howell and Mario H. Rheinfurth		8. PERFORMING ORGANIZATION REPORT #
9. PERFORMING ORGANIZATION NAME AND ADDRESS George C. Marshall Space Flight Center Marshall Space Flight Center, Alabama 35812		10. WORK UNIT NO. M-395
		11. CONTRACT OR GRANT NO.
12. SPONSORING AGENCY NAME AND ADDRESS National Aeronautics and Space Administration Washington, D.C. 20546		13. TYPE OF REPORT & PERIOD COVERED Technical Paper
		14. SPONSORING AGENCY CODE

15. SUPPLEMENTARY NOTES

Prepared by Systems Dynamics Laboratory, Science and Engineering Directorate.

16. ABSTRACT

The generation of pseudo-random numbers from specified probability distributions has found extensive application in Monte Carlo simulations. Because these simulations often require a large number of calculations, the time required to generate pseudo-random numbers has become a major factor. At the same time it is essential to guarantee accuracy and statistical randomness of the sequence of generated numbers. This report provides practical methods for generating acceptable random numbers from a variety of probability distributions which are frequently encountered in engineering applications.

17. KEY WORDS Random Number Generators Monte Carlo Simulations Pseudo-Random Numbers Congruential Sequences Uniform Random Numbers	18. DISTRIBUTION STATEMENT Unclassified - Unlimited STAR Cagetory: 65

19. SECURITY CLASSIF. (of this report)	20. SECURITY CLASSIF. (of this page)	21. NO. OF PAGES	22. PRICE
Unclassified	Unclassified	27	A03

For sale by National Technical Information Service, Springfield, Virginia 22161

NASA-Langley, 1982

National Aeronautics and Space Administration

Washington, D.C. 20546

Official Business

Penalty for Private Use, $300

THIRD-CLASS BULK RATE

Postage and Fees Paid
National Aeronautics and Space Administration
NASA-451

U.S. MAIL

4 1 1U,G, 821206 S00903DS
DEPT OF THE AIR FORCE
AF WEAPONS LABORATORY
ATTN: TECHNICAL LIBRARY (SUL)
KIRTLAND AFB NM 87117

S

NASA

POSTMASTER: If Undeliverable (Section 158 Postal Manual) Do Not Return